Claims

1. A security module for use with a terminal, comprising

a data interface adapted to be coupled to a terminal, for receiving at least part of an **algorithm code** or of the complete **algorithm code** from the terminal, with the algorithm code concerning a processing of secrets,

an energy interface for receiving supply energy from the terminal;

a volatile memory for storing the part of the **algorithm code** or the complete **algorithm code** received via the data interface, said volatile memory being coupled to the energy interface in order to have energy supplied thereto such that the same will be cleared upon an interruption of the receipt of the supply energy from the terminal; and

a processor for performing the **algorithm code** in order to obtain an **algorithm code** result that can be delivered to the terminal.

2. A security module, further comprising:

a non-volatile memory in which the non-received remainder of the **algorithm code** is stored.

3. A security module according to claim 1, further comprising:

a means for performing an authentication between the terminal and the **security module**.

4. A security module according to any of claim 1, wherein the data interface is arranged to receive from the terminal said part of the **algorithm code** or the complete **algorithm code** in encrypted form and/or a certificate, with the **security module** further comprising:

a means for decrypting said part of the encrypted **algorithm code** or the encrypted complete **algorithm code**; and

a means for examining the certificate and for preventing performing of the **algorithm code** if said certificate lacks genuineness.

5. A security module according to any of claim 1, further comprising:

a memory managing unit for controlling memory accesses of the processor, with the transferred part of the **algorithm code** containing addresses of the **algorithm code**.

6. A security module according to any of claim 1, further comprising:

a means for monitoring a predetermined security condition and for clearing the volatile memory if said predetermined security condition is fulfilled, with said security condition being selected from a plurality of conditions comprising an interruption, an irregularity and a fluctuation of the supply voltage and of a system clock as well as of additional operating parameters.

7. A security module according to any of claim 1, wherein the **algorithm code** comprises a program code selected for carrying out a task selected from a group comprising a symmetric cryptographic algorithm, an

asymmetric cryptographic algorithm, an RSA algorithm, a cryptographic process according to the DES standard, an elliptic curve process and an access function for accessing as well as an access function for changing a value stored on the security module.

8. A security module according to any of claim 1, wherein the part received of the algorithm code comprises a start address of the algorithm code, memory addresses of computing components necessary for performing the algorithm code, or jump addresses of the algorithm code.

9. A security module according to any of claim 1, wherein the volatile memory is arranged for storing a newly received, altered part of the algorithm code over the stored part of the algorithm code or the stored complete algorithm code.

10. A security module according to any of claim 1, wherein said security module is designed as a chip card.

11. A process for computing an algorithm code result using a security module, comprising the steps of:

receiving at least part of an algorithm code or the complete algorithm code by means of an energy interface, with the algorithm code concerning a processing of secrets;

volatile-storing said part of the algorithm code or said complete algorithm code in a volatile memory of the security module, with the volatile memory being coupled to the energy interface, to be supplied with energy, such that the same will be cleared upon an in-

terruption of the receipt of the supply energy from the terminal:

performing said algorithm code on the security module in order to obtain an algorithm code result;

delivering said algorithm code result to the terminal; and

clearing said volatile memory upon an interruption of the receipt of the supply energy from the terminal.

12. A process according to claim 11, wherein said step of clearing comprises removing the security module from the terminal.

13. A terminal for use with a security module, comprising:

a data interface adapted to be coupled to the security module, for transmitting at least part of an algorithm code or the complete algorithm code from the terminal to a volatile memory of the security module and for receiving the algorithm code result from the security module, with the algorithm code concerning a processing of secrets; and

an energy interface for delivering supply energy to the security module, with the volatile memory being supplied by the supply energy, such that the same will be cleared upon an interruption of the receipt of the supply energy from the terminal,

with the terminal, for each communication operation between terminal and security module during one and the same communication operation with the security module, being designated to

send at least the part of the algorithm code or the complete algorithm code to the volatile memory of the security module; and,

subsequently, during the further communication process, receive the algorithm code result from the security module.

14. A process for controlling a security module using a terminal in order to obtain an algorithm code result from the security module, with the process comprising for each communication operation, performing the following steps during one and the same communication operation with the security module:

delivering supply energy from the terminal to the security module;

transmitting at least part of an algorithm code or the complete algorithm code from the terminal to a volatile memory of the security module, with the algorithm code concerning a processing of secrets, with the volatile memory being supplied by the supply energy, such that the same will be cleared upon an interruption of the receipt of the supply energy from the terminal; and

receiving the algorithm code result from the security module.

15. A process for communication between a security module and a terminal, comprising the steps of:

transferring at least part of an algorithm code or the complete algorithm code from the terminal to the security module, with the algorithm code concerning a processing of secrets;

volatile-storing said part of the algorithm code or said complete algorithm code in a volatile memory of the security module, with the volatile memory being supplied by the supply energy, such that the same will be cleared upon interruption of the receipt of the supply energy from the terminal;

performing said algorithm code on the security module in order to obtain an algorithm code result;

delivering said algorithm code result to the terminal; and

clearing said volatile memory upon an interruption of the receipt of the supply energy from the terminal.

16. A process according to claim 15, further comprising:

repeated transferring of a plurality of different versions of said part of the algorithm code or said complete algorithm code; and

storing the repeatedly transferred version of said part of the algorithm code or of the complete algorithm code over the stored part of the algorithm code or over the complete stored algorithm code.